PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04N

A2

(11) International Publication Number: WO 00/59203

(43) International Publication Date: 5 October 2000 (05.10.00)

(21) International Application Number: PCT/US00/08541

(22) International Filing Date: 30 March 2000 (30.03.00)

(30) Priority Data:

60/127,128	31 March 1999 (31.03.99)	US
60/127,122	31 March 1999 (31.03.99)	US
09/458,620	10 December 1999 (10.12.99)	US

(71) Applicant: DIVA SYSTEMS CORPORATION [US/US]; 800 Saginaw Drive, Redwood City, CA 94063 (US).

(72) Inventor: BERTRAM, Michael, C.; 417-17 Camille Circle, San Jose, CA 95134 (US).

(74) Agents: MOSER, Raymond, R. et al.; Thomason Moser and Patterson LLP, 2-40 Bridge Avenue, P.O. Box 8160, Red Bank, NJ 07701 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

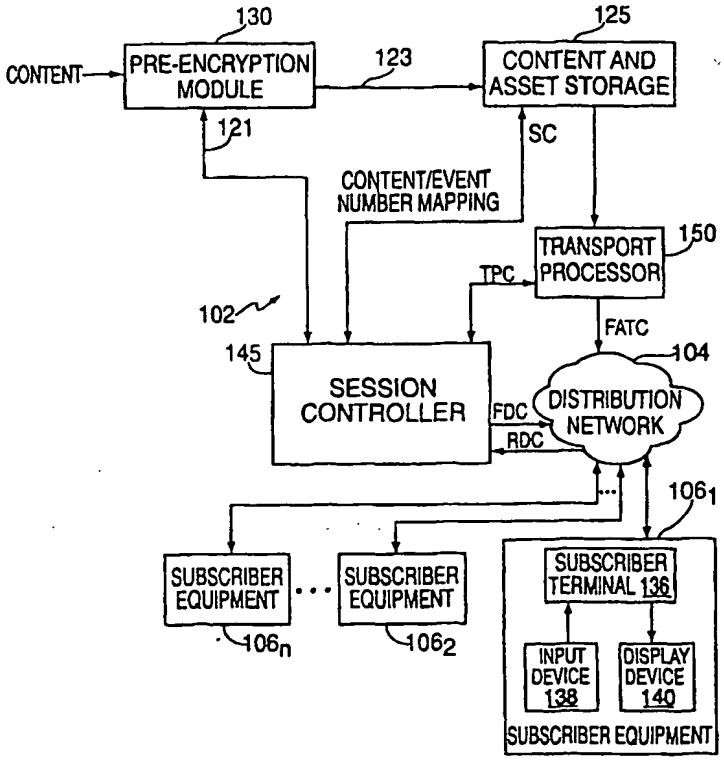
Published

Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD AND APPARATUS FOR PERFORMING IMPULSE AUTHORIZATIONS WITHIN A VIDEO ON DEMAND ENVIRONMENT

(57) Abstract

A method and apparatus for enabling conditional access to on-demand content of variable duration by utilizing either real time encryption of the content or pre-encryption of the content. In either case, embedding decryption messages and impulse authorizations are included with the pre-encrypted information stream.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

BNSDOCID: <WO__0059203A2_I_>

METHOD AND APPARATUS FOR PERFORMING IMPULSE AUTHORIZATIONS WITHIN A VIDEO ON DEMAND ENVIRONMENT

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims benefit of U.S. Provisional Patent Applications Serial Number 60/127,128 (attorney docket number 036) and 60/127,122 (attorney docket number 042), both filed on March 31, 1999, both of which are incorporated herein by reference in their entireties.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to an information distribution system such as a video-on-demand (VOD) system. More particularly, the present invention relates to a method and apparatus for applying conditional access impulse authorization techniques to information on demand services such as video on demand services.

2. Description of the Background Art

In an information distribution system, such as video on demand (VOD) system, an information provider (e.g., a head-end in a cable television system) must control of the distribution of requested information to ensure that only an appropriate information consumer (e.g., a requesting VOD subscriber) is able to utilize the distributed information. To provide this functionality, information distribution systems are often implemented using a conditional access system.

VOD systems providing content encoded according to the various Moving Pictures Experts Group (MPEG) standards are known. For example, a first standard known as MPEG-1 refers to ISO/IEC standards 11172, which is incorporated herein by reference in its entirety. A second standard known as MPEG-2 refers to ISO/IEC standards 13818, which is

incorporated herein by reference in its entirety. Additionally, a compressed digital video system is described in the Advanced Television Systems Committee (ATSC) digital television standard document A/53, incorporated herein by reference.

MPEG-based conditional access systems typically have three main attributes: the scrambling (or encoding) of MPEG streams, the transmission of de-scrambling messages and the transmission of authorization messages. De-scrambling messages are embedded in the MPEG transport stream and used by information consumer equipment (e.g., set top terminals) to descramble the content. Authorization messages can be sent with the scrambled stream or by some other route and are used to authorize set top terminals to use the descrambling information.

Most conditional access systems support addressing authorization messages to a pre-defined individual set top terminal (STT) or groups of STTs. That is, the head end controls which set top terminals receive the authorization messages. This method is primarily used to support conditional access for premium services (such as HBO) and call ahead pay per view.

Some conditional access systems support the concept of impulse authorizations. Impulse authorizations are primarily used for pay per view events. In the impulse method of authorization, non-STT specific authorization messages are sent to all set top terminals. The set top terminal determines if the authorization message is to be used (based upon input to the STT indicative of the desires of a viewer). Thus, the head-end of such a VOD system does not know which STTs will use the authorization. Each STT using the authorization must report such use to the head-end in some manner to ensure proper billing for content that has already been presented to the viewer.

Existing conditional access systems use a schedule including a start time, an end time, channel location, and an event number to control the scrambling, transmission of descrambling messages, and transmission of impulse authorization messages identified by the event number. In parallel, set top terminals are provided with a list of pay per view events as, e.g., a menu or electronic programming guide. Each of those pay per view events

has an associated event number matching the number provided to the conditional access system. When a viewer orders a pay per view event, the set top box uses the associated event number to find the appropriate impulse authorization.

Video on demand does not fit this model because the start time, the end time, and the channel location of events are typically not known in advance.

Therefore, it is seen to be desirable to provide a method and apparatus enabling conditional access to on-demand content of variable duration. Moreover, it is seen to be desirable to provide such conditional access using impulse authorizations. More generally, it is seen to be desirable to apply such impulse authorization techniques to content such that requested content may be real-time encrypted or pre-encrypted.

SUMMARY OF THE INVENTION

The disadvantages heretofore associated with the prior art are overcome by the present invention of a method and apparatus for enabling conditional access to on-demand content of variable duration by utilizing either real time encryption of the content or pre-encryption of the content. in either case, embedding decryption messages and impulse authorizations are included with the pre-encrypted information stream. Another embodiment of the invention utilizes real time encryption of the content

Specifically, in a conditional access protected information distribution system, a method according to the invention comprises the steps of: encrypting an information stream having associated with it an event identifier to produce an encrypted information stream; embedding, in the encrypted information stream, a descrambling message and an impulse authorization to produce a pre-encrypted stream; storing the pre-encrypted stream; and providing the pre-encrypted stream to an information consumer, the embedded descrambling message and impulse authorization enabling decryption of the pre-encrypted stream by the information consumer.

Additionally, in a conditional access protected information distribution system including information provider equipment and

information consumer equipment, information provider apparatus according to the invention comprises: a pre-encryption module, for encrypting an information stream having associated with it an event identifier to produce an encrypted information stream, and for embedding, in the encrypted information stream, a descrambling message and an impulse authorization to produce a pre-encrypted stream; a storage device, for storing the pre-encrypted information stream; and a session controller, for retrieving the pre-encrypted information stream from the storage device and causing the pre-encrypted information stream to be communicated to an information consumer requesting the pre-encrypted information stream, the embedded descrambling message and impulse authorization enabling decryption of the pre-encrypted stream by the information consumer.

In a conditional access information distribution system, a method according to another embodiment of the invention comprises the steps of: receiving, from the set top terminal, a request for content; scrambling content provided to the requesting set top terminal via a defined channel; inserting descrambling messages and impulse authorizations for the requested content into the defined channel; and providing the requested content to the set top terminal via the defined channel, the requested content being scrambled prior to transmission via the defined channel.

BRIEF DESCRIPTION OF THE DRAWINGS

The teachings of the present invention can be readily understood by considering the following detailed description in conjunction with the accompanying drawings, in which:

FIG. 1 depicts a high level block diagram of an interactive information distribution system;

FIG. 2 depicts a block diagram of the set top terminal suitable for use in the interactive information distribution system of FIG. 1;

FIG. 3 depicts a flow diagram of a content processing method suitable for use in the system of FIG. 1;

FIG. 4 depicts a flow diagram of an illustrative implementation of an impulse authorization method as performed on both service provider

BNSDOCID: <WO__0059203A2_I_>

equipment and subscriber equipment within the interactive information distribution system of FIG. 1;

FIG. 5 depicts a high level block diagram of an alternate embodiment of the interactive information distribution system of FIG. 1; and

FIG. 6 depicts a flow diagram of an illustrative implementation of an impulse authorization method as performed on both service provider equipment and subscriber equipment within the interactive information distribution system of FIG. 5.

To facilitate understanding, identical reference numerals have been used, where possible, to designate identical elements that are common to the figures.

DETAILED DESCRIPTION

Throughout this description various terms are used to describe the invention. Unless modified by the following description, several of the terms are defined as follows: Scrambling comprises a method of protecting a data stream by transforming the value of bits in the stream based on a given key. For the purposes of this disclosure scrambling has the same meaning as encrypting. Descrambling comprises a method for transforming data stream bits back to their original value based on the use of a key. For the purposes of this description disclosure has the same meaning as decryption. A conditional access (CA) system is a system that generates keys, descrambling messages, and impulse authorization messages supporting the scrambling and descrambling of, e.g., MPEG encoded programs. A descrambling message comprises a conditional access message containing descrambling information for a particular MPEG program. The descrambling information may be the descrambling key or the information a Set Top Box (or boxes) needs to generate the descrambling key. An impulse authorization message comprises a conditional access message authorizing Set Top Boxes to use a descrambling key to descramble a particular MPEG program.

FIG. 1 depicts a high level block diagram of an interactive information distribution system. Specifically, FIG. 1 depicts a high level block diagram of an interactive information distribution system 100

containing the present invention and suitable for applying impulse authorization techniques using pre-encrypted content. The system 100 contains service provider equipment 102, a communications network 104 and subscriber equipment 106_n, where n is an integer greater than zero.

The service provider equipment 102 comprises a content and asset storage module 125, a pre-encryption module 130, a session controller 145 and a transport processor 150. Briefly, the session controller 145, in response to a request from subscriber equipment 106, causes requested content and associated assets to be retrieved from the content and asset storage module 125 and provided to the transport processor 150. The transport processor 150 combines or multiplexes the content and asset data to provide an output data stream for the requesting subscriber. The output data stream is conditioned for transport to the requested subscriber via a forward application transport channel (FATC) within the distribution network 104.

The content and asset storage module 125 is used to store content such as movies, television programs and other information offerings of the interactive information distribution system 100 of FIG. 1. Additionally, the content and asset storage module 125 is used to store assets such as bit map imagery, graphic overlay, control scripts and the like. The assets may comprise, for example, navigation assets that are used by a set top terminal to interactively navigate, and select for viewing, the offerings or content available from the service provider equipment 102. The content and asset storage module 125, in response to a control SC produced by the session controller 145, provides content and/or asset data to the transport processor 150.

The session controller 145 (or session controller) provides session control of the information flowing to and from the content and asset storage module 125, and may be generally described as a system providing or controlling communications between, for example, a cable system head-end and one or more set top terminals. The session controller 145 produces the storage control signal SC for controlling and communicating with the content and asset storage module 125, and a transport processor control signal TPC for controlling and communicating with the transport processor

150. In response to a user request for particular content, the session controller 145 causes the requested content file and any associated assets to be streamed from the content and asset storage module 125 to the transport processor 150.

The session controller 145 sends data, such as commands to set top terminals via a forward data channel (FDC). The session controller 145 receives data, such as information stream requests and session initiation data (set top identification, capability and the like) via a reverse data channel (RDC). The FDC and RDC are supported by the distribution network 104 and comprise relatively low bandwidth data channels, such as one-two megabits per second data channels utilizing QPSK, QAM, or other modulation techniques. The FDC and RDC are also known as "out-of-band" channels, while the relatively high bandwidth forward application transport channel (FATC) is also known as an "in-band" channel. The session controller 145 contains an interface device for sending control information via the forward data channel FDC and receiving control information and request information via the reverse data channel RDC using the so-called "out-of-band" carrier frequencies.

The transport processor 150 accomplishes all of the forward content channel transmission interface requirements of the system 100 of FIG. 1. Specifically, the transport processor 150 is coupled to subscriber equipment via the forward applications transport channel (FATC). That is, the transport processor 150 is capable of providing a plurality of scrambled or unscrambled content and/or asset streams modulated onto various carrier frequencies suitable for use in the distribution network 104. The FATC is supported by the distribution network 104 and comprises a relatively high bandwidth communications channel well suited to carrying video, audio and data such as, for example, multiplexed MPEG-2 transport packets. It should be noted that data normally conveyed to a set top terminal via the FDC may be included in the FATC data stream. The transport processor 150 also contains a modulator for modulating the combined content and asset stream onto one or more carrier frequencies for transmission on the FATC, the so-called "in-band" carrier frequencies.

The pre-encryption module 130 receives content, associates the content with an event number, encrypts the content from a content development facility (not shown), and embeds descrambling messages and impulse authorization messages into the encrypted content stream to form a so-called "pre-encrypted" content stream. The pre-encrypted content stream is stored in the content and asset storage module 125, from which it can be retrieved for subsequent transport to a STT in response to a request from the STT (e.g., a video on demand request). The pre-encryption module 130 provides, via signal path 121, the session controller 145 with an event identification that associates the encrypted content with the impulse authorization. The operation of the pre-encryption module 150 will be discussed in more detail below with respect to FIGS. 3 and 4.

The distribution network 104 can be any one of a number of conventional broadband communications networks that are available such as a fiber optic network, a telephone network, existing cable television network and the like. For example, if the network is a hybrid fiber-coax network, the transmission transport technique used in both forward channels may be modeled after the Moving Pictures Expert Group (MPEG) transport protocol for the transmission of video data streams. In general, the transport mechanism for both of the forward channels that transport information to the set top terminal must be able to carry unidirectional, asynchronous packetized data such as that defined in the MPEG video and audio signal transmission protocol, and the like. There are a number of such transport protocols available.

The subscriber equipment 106 comprises a set top terminal or a set top box 136, a display device 140 (e.g. a conventional television) and a user input device 138 (e.g. a remote control device). Each set top terminal 136 receives the data streams from the FATC, demodulates the received data streams and, in the case of video streams, processes the demodulated video streams for subsequent display on the display device 140. In the case of receiving scrambled data streams, the STT descrambles the received data streams using the descrambling messages DM provided to the STT via the FATC. The STT uses the impulse authorization messages IAM provided via the FATC to gain the authorization needed to use the descrambling

messages. In addition, the set top terminal 136 accepts commands from the remote control input device 138 or other input device. These commands are formatted, modulated, and transmitted through the distribution network 104 to the session controller 145. Typically, this transmission is accomplished through the reverse data channel RDC. These commands are preferably transmitted through the same network used to transmit information to the set top terminal. However, the RDC coupling the set top terminal to the provider equipment 102 may be a separate network, e.g. a FATC through a television cable network and an RDC through a telephone network. The telephone network could also support the FDC.

FIG. 2 depicts a block diagram of the set top terminal (STT) suitable for use in the interactive information distribution system of FIG. 1. A set top terminal (or set top box) comprises a device capable of receiving and decompressing content within, e.g., an MPEG transport stream to produce a resulting signal(s) suitable for use by a presentation device such as a display device. Set top terminals are also capable of conditional access message processing and transport stream descrambling.

Specifically, FIG. 2 depicts a block diagram of an exemplary embodiment of the set top terminal 136 interactive information distribution system of FIG. 1. The STT 136 of FIG. 2 comprises a transceiver 200, a central processing unit (CPU) 212 and a display driver 222. The CPU 212 is supported by random access memory (RAM) 220, read only memory (ROM) 218 and various support circuits 216 such as clocks, power supply, an infrared receiver and the like. The transceiver 200 contains a diplexer 202, a back channel transmitter 208, an information channel receiver 204, a conditional access module 205, a command channel receiver 210 and an transport demultiplexer and decoder 206. The diplexer 202 couples the three channels carried by a single cable within the network to the transmitter and receivers.

Each receiver 204 and 210 contains a tuner, amplifiers, filters, a demodulator, and a depacketizer. As such, the receivers tune, downconvert, and depacketize the signals from the cable network in a conventional manner. The information channel receiver 204 contains a conventional QAM demodulator such as a model BCM3115 manufactured by the

Broadcom Corporation. Other such demodulators are well-known in the communications arts and could be used in this application. However, this particular QAM demodulator also contains a built in "out-of-band" QPSK demodulator for handling data carried by the forward data channel FDC. As such, a single integrated circuit demodulates both subscriber requested information (audio and video) as well as command data.

The transport demultiplexer and decoder 206 processes the data packets carrying subscriber requested information produced by the QAM demodulator into useable signals for the end user display, e.g., television, home studio, video recorder and the like. The decoder is coupled to a dynamic random access memory (DRAM) to facilitate decoding of the data packets and processing of applets, as shall be discussed below. The signals for display are conventionally processed by a display driver 222 to produce a video signal suitable for use by, e.g., the display device 140.

The transport demultiplexer and decoder 206 also extracts authorizations and descrambling messages from the received data stream and provides the extracted authorizations and descrambling messages to the conditional access module 205.

The conditional access module 205, illustratively a smart card, accepts authorizations and descrambling messages extracted by the transport demultiplexer and decoder 206 and responsively provides descrambling keys for the selected content stream.

The transport demultiplexer and decoder 206 utilizes the descrambling keys provided by the conditional access module 205 to descramble or decrypt the selected content stream prior to decoding the stream to form appropriate presentation signals.

The demodulated QPSK signal provides command and control information to the CPU 212 for generating a graphical user interface upon the display device 140. The CPU 212, operating in combination with the transport demultiplexer and decoder 206, as well as a continuously available video signal from the information receiver 204, produces screen displayed buttons, icons and graphical regions with which a subscriber interacts using the remote control 138. User interaction comprises, e.g., the navigation of a

BNSDOCID: <WO___0059203A2_I_>

graphical user interface to select one of a plurality of available program titles for immediate or future presentation.

Session control commands are implemented by the session controller 145 and not the set top terminal 136 alone. Each command is implemented by the execution of an applet by the set top terminal 136. The applet is transmitted to the STT by the session controller 145 in response to, for example, requests transmitted by the STT via the RDC. The applets control both information sessions, for example, the presentation of video to the television screen, and navigator functions, for example, the menus that facilitate selection of a video program. As such, particular commands include, but are not limited to, information or menu navigation commands, movie start at beginning, movie start at the middle, play, stop, rewind, forward, pause, and the like. These presentation and navigation control commands are sent via a back channel transmitter 208 using binary phase shift key (BPSK) modulation.

As previously noted, the pre-encryption module 130 receives the content, associates the content with an event number, encrypts the content, and embeds descrambling messages and impulse authorization messages into the encrypted content stream to form a so-called "pre-encrypted" content stream. The pre-encrypted content stream is stored in the content and asset storage module 125, from which it can be retrieved for subsequent use by the session controller 145 in response to a request from a set top terminal (e.g., a video on demand request).

The session controller 145 controls the output of the content and asset storage module 125 via the control signal SC. The session controller 145 receives information from the pre-encryption module 160, such as content and event number mapping information, via signal path 121. The session controller 145 receives session control messages, content requests and other information from the subscriber equipment 106 via the RDC. The session controller 145 transmits session control messages, event numbers and other information to the subscriber equipment 106 via the FDC or, optionally, the FATC. The pre-encryption module 160 couples pre-encrypted content to the content and asset storage module 125 via signal path 123. The transport processor 150 processes content and/or asset data and modulates the

processed data onto a carrier frequency associated with a physical channel intended to be tuned by a STT requesting the content and/or asset data.

FIG. 3 depicts a flow diagram of a content processing method suitable for use in the system of FIG. 1. Specifically, FIG. 3 depicts a method 300 suitable for use by the pre-encryption module 130 of the interactive information distribution system 100 of FIG. 1.

The method 300 of FIG. 3 is entered at step 302 where an event number is associated with received content. That is, an information stream (e.g., a digital video stream and a related audio stream) providing content such as a movie, television show, sporting event or other audio visual or informational presentation is received by the pre-encryption module 130 and associated with an event number. The event number is an alpha-numeric or other identifier for uniquely identifying a particular event. The event number associated with the received content is also communicated to the session controller 145 for subsequent session processing between the session controller 145 and subscriber equipment 106.

At step 304 the content stream is encrypted. That is, the content is scrambled or encrypted according to a scrambling or encrypting algorithm to produce a scrambled or encrypted content stream.

At step 306 descrambling messages and impulse authorizations are embedded into the encrypted content stream. The descrambling messages comprise a conditional access message containing the descrambling information for a particular content stream, such as an MPEG program. The descrambling information may be the descrambling key or the information a set top terminal or subscriber equipment needs to generate the descrambling key.

The impulse authorization is a conditional access message usable by any set top terminal to allow that set top terminal to use a descrambling key to descramble a particular content stream, such as an MPEG program. Thus, the encrypted content stream includes a descrambling key (or information necessary to generate such a descrambling key) and an authorization to use the descrambling key. It is critical to note that the descrambling messages and impulse authorizations are embedded in the encrypted content such that any streaming of that content to a subscriber

BNSDOCID: <WO___0059203A2_I_>

inherently includes the providing of the descrambling messages and impulse authorizations to that subscriber.

At step 308 the encrypted content including the embedded descrambling messages and impulse authorizations is loaded onto a server or other data storage device, such as the content and asset storage module 125 of the system 100 of FIG. 1.

FIG. 4 depicts a flow diagram of an illustrative implementation of an impulse authorization method as performed on both the service provider equipment and subscriber equipment. Specifically, FIG. 4 is divided into two columns, namely: a service provider equipment process column 402 and a subscriber equipment process column 404.

In the above manner, content is scrambled and the impulse authorization messages are embedded once, before the content is loaded onto the content and asset storage module 125. It should be noted that these functions may also be performed during, e.g., transmission of the content to one or more set top terminals.

The method 400 of FIG. 4 begins at steps 406 and 407 where, respectively, the service providers equipment and subscriber equipment establish a session with each other.

At step 408 the service provider equipment identifies or defines a channel identifier (e.g., a physical and logical transmission channel) and communicates the defined channel identifier to the subscriber equipment. The subscriber equipment receives the defined channel identifier at step 409.

At step 410 the subscriber equipment requests desired content from the service provider equipment. At step 412 the service provider equipment receives the content request from the subscriber equipment.

At step 414 the service provider equipment determines the event identifier (e.g., an event number) for the requested content and communicates the event number to the subscriber equipment. At step 416 the subscriber equipment receives the event number for the requested content from the service provider equipment.

At step 418 the subscriber equipment tunes the defined channel, illustratively, a QAM channel comprising one or more transport streams

including video and audio streams associated with the requested content. At step 420 the service provider equipment begins streaming the requested content and the embedded messages and authorizations to the subscriber equipment via the defined channel.

At step 418 the subscriber equipment tunes the defined channel and begins to extract the streamed content and embedded messages and authorizations provided by that channel.

At step 422 the subscriber equipment waits for an impulse authorization matching the defined event number. That is, the set top box, having tuned to the channel indicated during the session setup, monitors the incoming data looking for an impulse authorization matching the event number provided by the session controller 145. When the set top box sees an impulse authorization matching the event number, it stores that authorization for use. The set top box will then use that impulse authorization, along with the embedded descrambling messages for that channel, to descramble and present the content to the viewer.

At step 424, upon receiving an impulse authorization matching the defined event number (per step 422), the impulse authorization is stored within the subscriber equipment memory. At step 426 the stored impulse authorization is used along with the embedded descrambling messages within the streamed content to descramble and present the desired content. That is, at step 426 the subscriber equipment utilizes the embedded impulse authorization and descrambling messages within the streaming content to descramble that content and present the descrambled content on, e.g., a display device.

At step 428, upon concluding the presentation of the desired content, the subscriber equipment requests that the session be terminated. At step 430 the service provider equipment receives a session termination request from the subscriber equipment. At step 432 the service provider equipment stops streaming the requested content and embedded messages and impulse authorizations. At step 434 the service provider equipment releases the defined channel such that the channel may be utilized by another session between the service provider equipment and another subscriber.

In the above described embodiment of the invention, it is noted that prior to the storing of any content in the content and asset storage module 125, the content is scrambled and descrambled messages and impulse authorizations are embedded in the resulting stream to form a pre-encrypted information stream. The scrambling and conditional access messages are based on a specified event number that is associated with the content by the pre-encryption module 130 and provided to the session controller 145. The scrambled content is then loaded onto the content and asset storage module 125 and made available for viewing by subscriber equipment 106.

The above-described methods and apparatus provide an non-standard use of impulse authorizations in which impulse authorizations are embedded within pre-encrypted content. As noted above, the pre-encrypted content is content that has been scrambled (encrypted) before storage on the server and includes descrambling messages and impulse authorizations needed by set top terminals to descramble the content.

Since the impulse authorizations are already embedded in the pre-encrypted content stream, the problems associated with regular (i.e., STT/STB-specific or non-impulse) authorizations are avoided. That is, the embedding of specific impulse authorizations during pre-encryption is not desirable (or possible) because it is not known in advance which set top terminals will be requesting specific pieces of content.

Additionally, since the content scrambling and insertion of conditional access messages occurs off-line (i.e., prior to streaming the content to a requesting subscriber), problems associated with unscheduled variable length events are bypassed. Using a definition whereby an event is defined both by the time the content starts and stops being scrambled and by the period of time where descrambling and authorization messages are valid and distributed, a pre-encrypted event exists any time that the server is streaming the content. Moreover, because the content has been pre-encrypted, it is always scrambled and the messages are always sent any time the server is streaming that piece of content.

FIG. 5 depicts a high level block diagram of an alternate embodiment of the interactive information distribution system of FIG. 1. Specifically,

FIG. 5 depicts a high level block diagram of an interactive information distribution system 500 containing an embodiment of the present invention and suitable for applying impulse authorization techniques using real-time encrypted content. Since the interactive information distribution system 500 of FIG. 5 is similar in many respects to the interactive information distribution system 100 of FIG. 1, only the differences between the two systems will be discussed in detail. These differences are primarily within the service provider equipment 102 of the system. The primary functional difference between the two systems is the use of off-line encryption (i.e., pre-encryption) by the system 100 of FIG. 1, and the use of real-time encryption (i.e., while streaming content to a requesting STT) by the system 500 of FIG. 5.

Specifically, the service provider equipment 102 of the system 500 of FIG. 5 does not include the pre-encryption module 130 found in the system 100 of FIG. 1. However, unlike the service provider equipment 102 of the system 100 of FIG. 1, the service provider equipment 102 of the system 500 of FIG. 5 includes a conditional access system 160. This and other differences will now be discussed in detail.

Referring to FIG. 5, the conditional access system 160, in response to an event request scrambling (ESR) signal produced by the session controller 145, generates scrambling keys SK, descrambling messages DM and authorization messages AM which are provided to the transport processor 150.

The transport processor 150 is capable of scrambling content and of inserting descrambling messages and impulse authorization messages IAM into a transport stream being provided to an output channel. The transport processor 150 utilizes the scrambling keys SK provided by the conditional access system 160 to scramble specific content, or content on a specific channel. The transport processor 150 embeds the descrambling messages DM and impulse authorization messages IAM provided by the conditional access system 160 (via the session controller 145) within the scrambled content or channel (that is, in-band communications to a requesting STT).

The transport processor 150 scrambles the retrieved content provided by the content and asset storage module 125 and inserts descrambling

messages and impulse authorization messages (IAM) into a transport stream including the scrambled content.

In a scrambling mode of operation, the session controller 145 provides the event scramble request (ESR) signal to the conditional access system 160 including the channel number or identifier of the channel to be scrambled (this channel identifier is also provided to the STT requesting the scrambled content stream). The event scramble request ESR signal also includes information indicative of the content and/or asset data to be scrambled, and which channel is to transport the scrambled content and/or asset data to the requesting STT.

FIG. 6 depicts a flow diagram of an illustrative implementation of a second embodiment of an impulse authorization method as performed on both the service provider equipment 102 and subscriber equipment 106 of FIG. 5. Specifically, FIG. 6 is divided into two columns, namely: a service provider equipment process column 602 and a subscriber equipment process column 604.

The method 600 of FIG. 6 begins at steps 606 and 607 where, respectively, the service providers equipment 102 and subscriber equipment 106 establish a session with each other.

At step 608 the service provider equipment 102 identifies or defines a channel identifier (e.g., a physical and logical transmission channel) and communicates the defined channel identifier to the subscriber equipment. The subscriber equipment receives the defined channel identifier at step 609.

At step 610 the subscriber equipment 100 requests desired content from the service provider equipment. At step 612 the service provider equipment receives the content request from the subscriber equipment.

At step 614 the service provider equipment determines the event identifier. The defined channel and event number is communicated to the subscriber equipment. At step 616 the subscriber equipment receives the channel and event number for the requested content from the service provider equipment. At step 618 the subscriber equipment tunes the defined channel, illustratively, a QAM channel received via the FATC comprising a transport stream including video and audio streams associated

with the requested content. At step 620 the service provider equipment begins streaming the requested content and the embedded messages and authorizations to the subscriber equipment via the defined channel.

At step 618 the subscriber equipment tunes the defined channel and begins to extract the streamed content and embedded messages and authorizations provided by that channel.

At step 622 the subscriber equipment waits for an impulse authorization matching the defined event number. That is, the set top box, having tuned to the channel indicated during the session setup, monitors the incoming data looking for an impulse authorization matching the event number provided by the session controller. When the set top box sees an impulse authorization matching the event number, it stores that authorization for use. The set top box will then use that authorization, along with the embedded descrambling messages for that channel, to descramble and present the content to the viewer.

At step 640 the provider equipment causes the conditional access system to begin generating messages and authorizations and the transport processor 150 to begin scrambling the information stream provided to the subscriber equipment via the defined channel. That is, the transport processor 150 scrambles the content to be provided to the channel intended to be used by a STT requesting scrambled content.

At step 642, the provider equipment causes the descrambling messages and impulse authorization messages (IAM) to be inserted into the transport stream provided to the defined channel. That is, the transport processor 150 inserts descrambling messages and impulse authorization messages (IAM) into the transport stream provided to the channel intended to be used by a STT requesting scrambled content.

At step 644, the provider equipment begins streaming the transport stream comprising the scrambled content and inserted (i.e., multiplexed) descrambling messages and impulse authorizations to the STT via the defined channel.

At step 624, upon receiving an impulse authorization matching the defined event number (per step 622), the impulse authorization is stored within the subscriber equipment memory. At step 626 the stored

BNSDOCID: <WO__0059203A2 I_>

authorization is used along with the embedded descrambling messages within the streamed content to descramble and present the desired content. That is, at step 626 the subscriber equipment utilizes the embedded authorization and descrambling messages within the streaming content to descramble that content and present the descrambled content on, e.g., a display device.

At step 628, upon concluding the presentation of the desired content, the subscriber equipment requests that the session be terminated. At step 630 the service provider equipment receives a session termination request from the subscriber equipment. At step 632 a service provider equipment stops streaming the requested content and injecting impulse authorization messages (IAM) and descrambling messages (DM). At step 634, the service provider equipment causes the conditional access system to stop scrambling content on the defined channel. At step 636 the service provider equipment releases the defined channel such that the channel may be utilized by another session between the service provider equipment and another subscriber.

It should be noted that while the steps comprising the methods 400 and 600 of, respectively, FIG. 4 and FIG. 6 are depicted as being in a particular order, variations of that order are contemplated by the inventor and are within the scope of the invention. For example, the steps of providing an identifier for a channel to transmit content (414;614) and receiving said channel identifier (416,616) may be included within the steps of establishing a session (406-407,606-608). Additionally, an information request may be made (410,610) and processed (412,612) before or after a channel is defined (414,614).

Although various embodiments which incorporate the teachings of the present invention have been shown and described in detail herein, those skilled in the art can readily devise many other varied embodiments that still incorporate these teachings.

What is claimed is:

1. In an information distribution system utilizing conditional access, a method comprising the steps of:

encrypting (304) an information stream having associated with it an event identifier to produce an encrypted information stream;

embedding (306), in said encrypted information stream, a descrambling message and an impulse authorization;

storing (308) said encrypted stream; and

providing (420) said encrypted stream to an information consumer, said embedded descrambling message and impulse authorization enabling decryption of said encrypted stream by said information consumer.

2. The method of claim 1, wherein said step of providing comprises the steps of:

identifying (414), in response to a request (412) for said encrypted stream by said information consumer, an event number associated with said encrypted stream and a transmission channel (408) for transmitting said pre-encrypted stream to said information consumer;

providing (416), to said information consumer, said identified event number and transmission channel; and

streaming (420), via said identified transmission channel, said pre-encrypted stream.

3. The method of claim 2, further comprising the steps of:

terminating (432) said step of streaming in response to a session termination request received from said information consumer.

4. The method of claim 1, further comprising the steps of:

providing (642), to said information consumer via at least one of a forward application transport channel (FATC) and a forward data channel (FDC), a descrambling key suitable for use in descrambling the encrypted information stream provided to said information consumer.

BNSDOCID: <WO___0059203A2_I_>

5. In an conditional access information distribution system, a method comprising the steps of:

receiving (612), from a set top terminal, a request for content;

scrambling (640) content provided to said requesting set top terminal via a defined channel;

inserting (642) descrambling messages and impulse authorizations for said requested content into said defined channel; and

providing (644) said requested content to said set top terminal via said defined channel, said requested content being scrambled prior to transmission via said defined channel.

6. The method of claim 5, wherein said descrambling messages and impulse authorizations are provided to said requesting set top terminal via a forward application transport channel.

7. The method of claim 5, wherein said descrambling messages and impulse authorizations are repeatedly provided to said set top terminal for a predefined amount of time.

8. The method of claim 5 further comprising the step of waiting to receive confirmation from said set top terminal of a receipt of said descrambling messages and impulse authorizations;

said step of scrambling being inhibited until said confirmation is received.

9. The method of claim 5 wherein said defined channel comprises a physical channel within a forward application transport channel carrying a transport stream including transport packets providing the requested content, said transport packets providing the requested content being associated with a particular logical channel.

10. In an information distribution system utilizing conditional access and including information provider equipment and information consumer equipment, information provider apparatus comprising:

a pre-encryption module (130), for encrypting an information stream having associated with it an event identifier to produce an encrypted information stream and for embedding in said encrypted information stream a descrambling message and an impulse authorization;

a storage device (125), for storing said encrypted information stream; and

a session controller (145), for retrieving said encrypted information stream from said storage device and for causing said encrypted information stream to be communicated to an information consumer requesting said encrypted information stream, said embedded descrambling message and impulse authorization enabling decryption of said encrypted information stream by said information consumer.

11. The apparatus of claim 10, further comprising:

a transport processor (150) responsive to said session controller, for adapting said encrypted information stream to a forward application transport channel (FATC), said information consumer retrieving said encrypted information stream from said FATC.

12. The apparatus of claim 10, wherein said session controller couples a descrambling key to said information consumer via at least one of a forward application transport channel (FATC).

13. The apparatus of claim 11 wherein said session controller couples a descrambling key to said information consumer via at least one of a forward application transport channel (FATC) and a forward data channel (FDC).

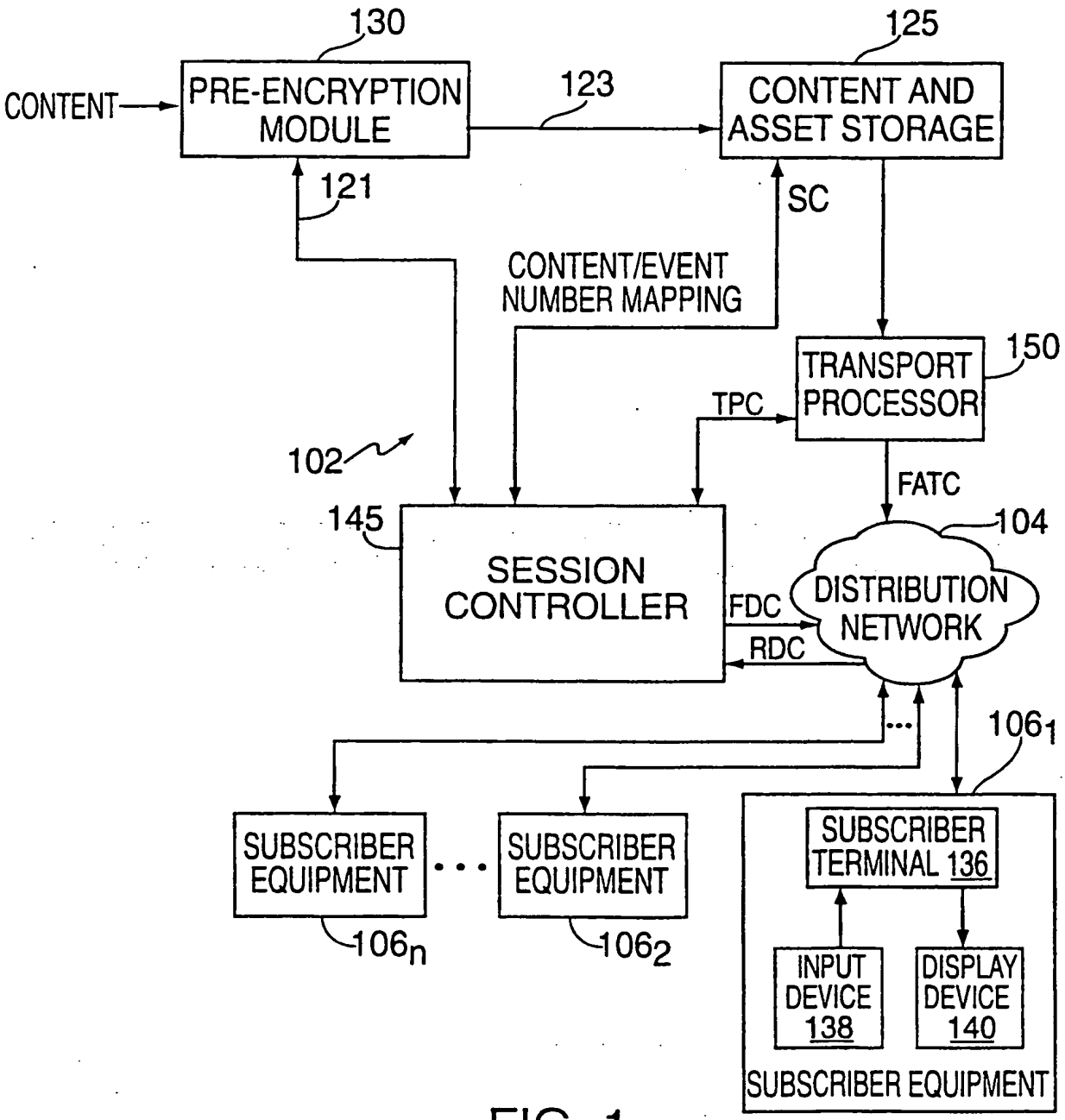


FIG. 1

BNSDOCID: <WO 0059203A2_I_>

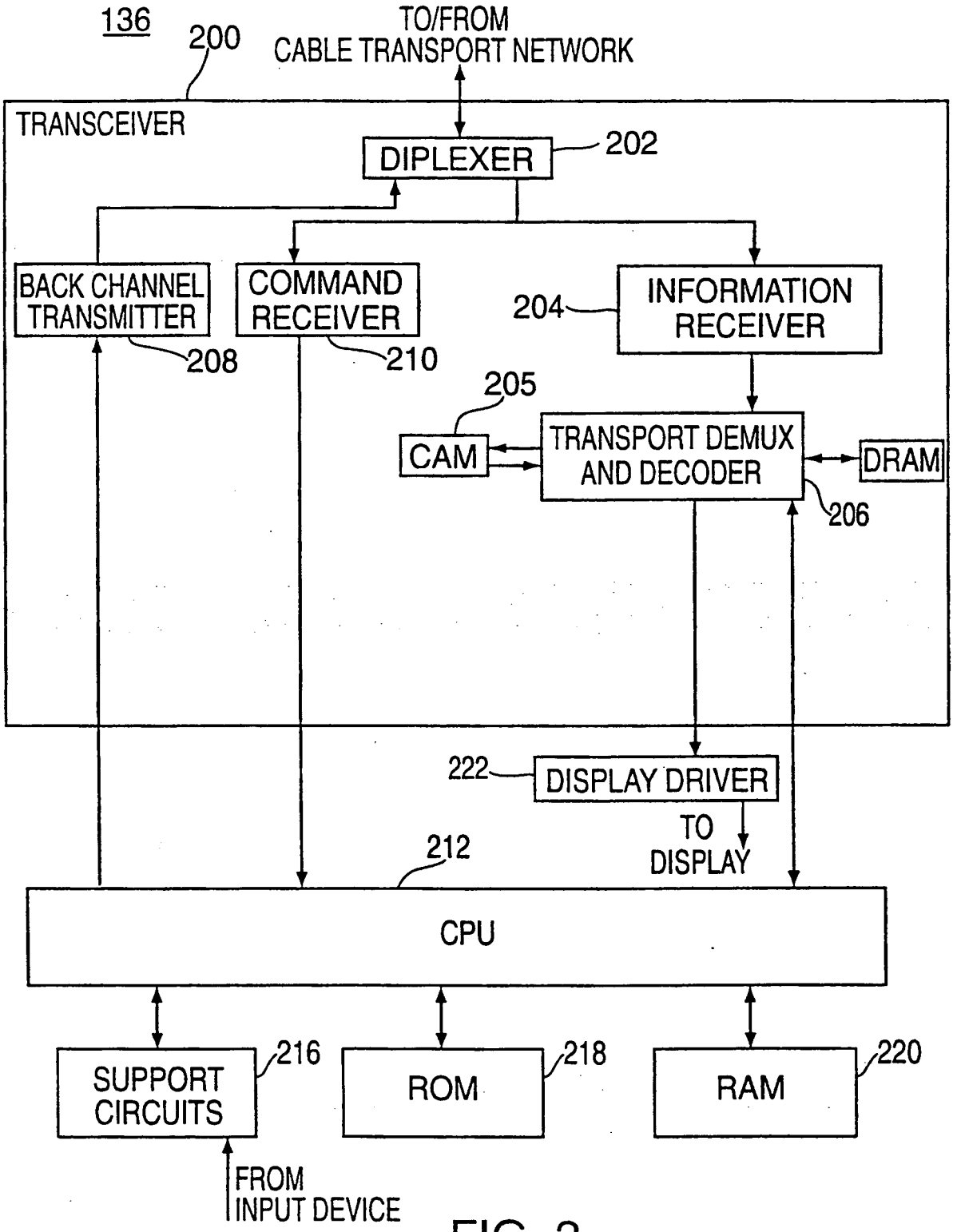


FIG. 2

BNSDOCID: <WO__0059203A2_I_>

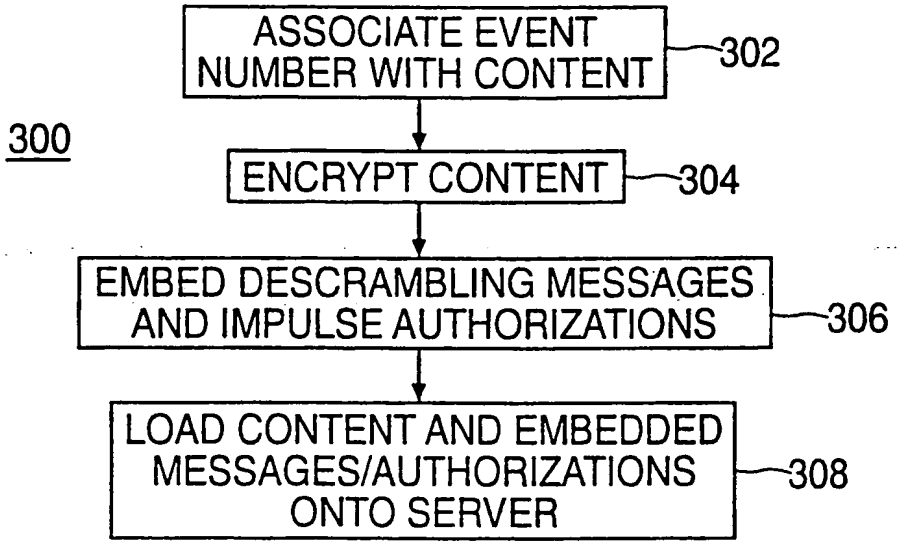


FIG. 3

BNSDOCID: <WO__ 0059203A2_I_>

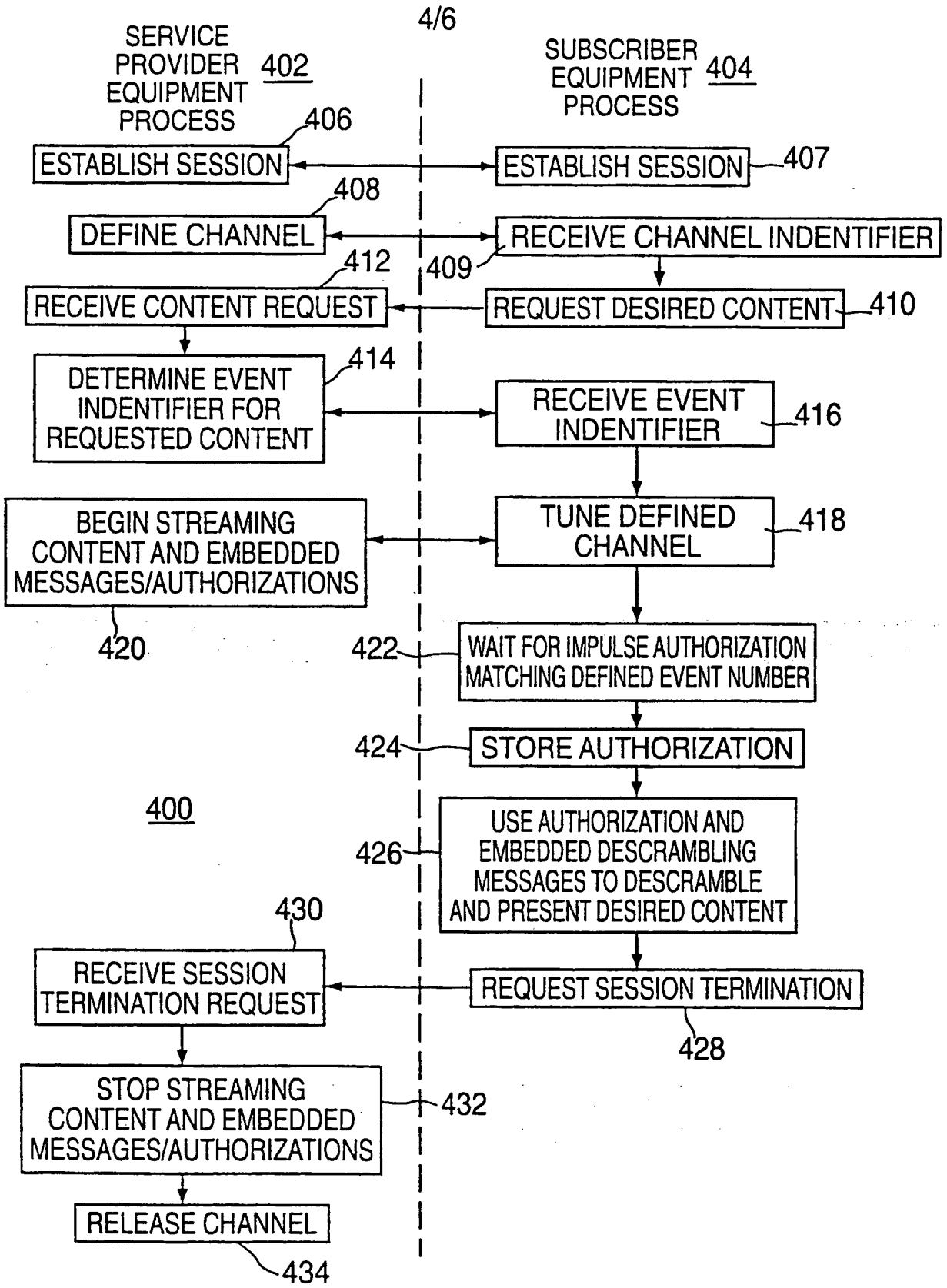


FIG. 4

BNSDOCID: <WO__ 0059203A2_I_ >

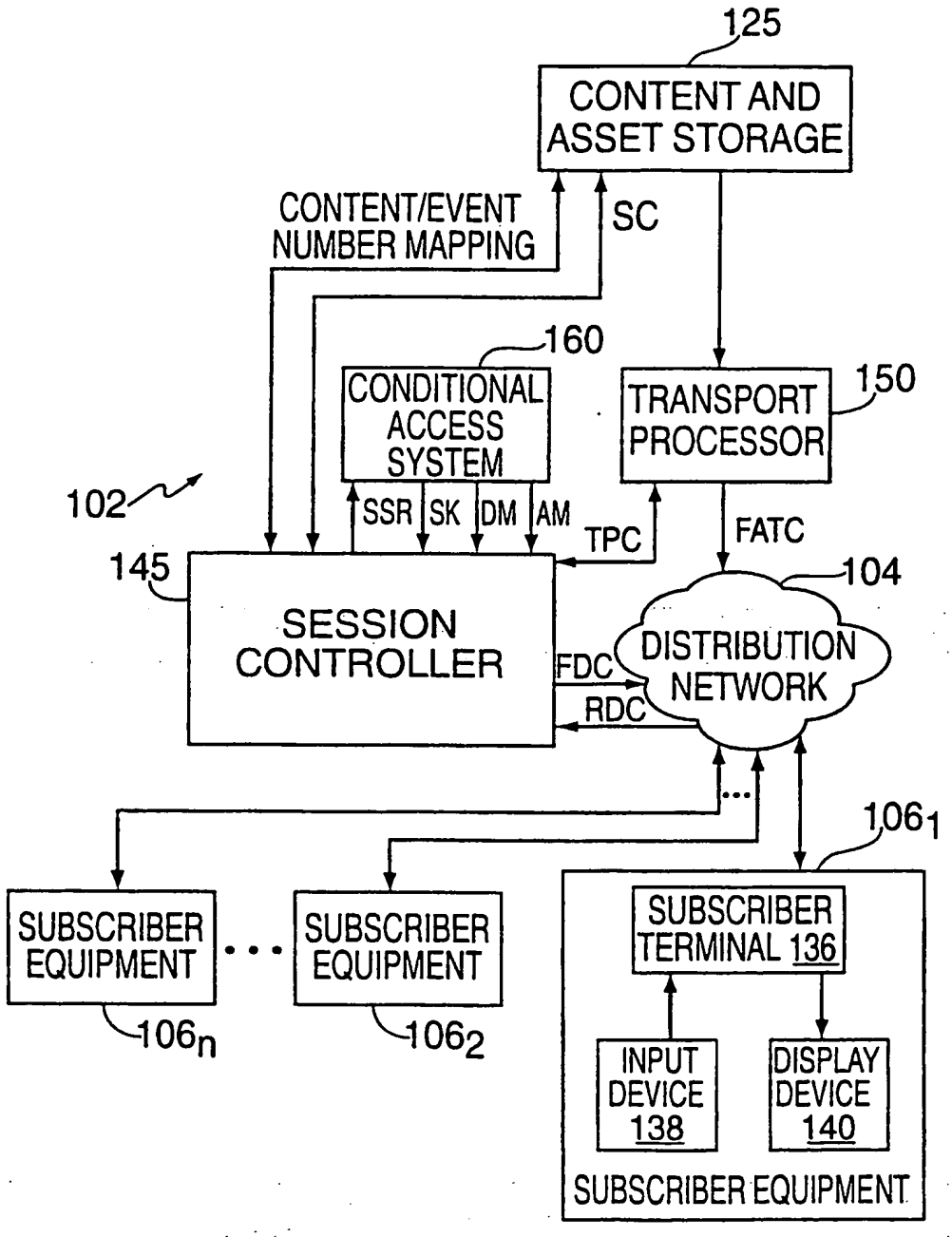


FIG. 5

BNSDOCID: <WO___0059203A2_I_>

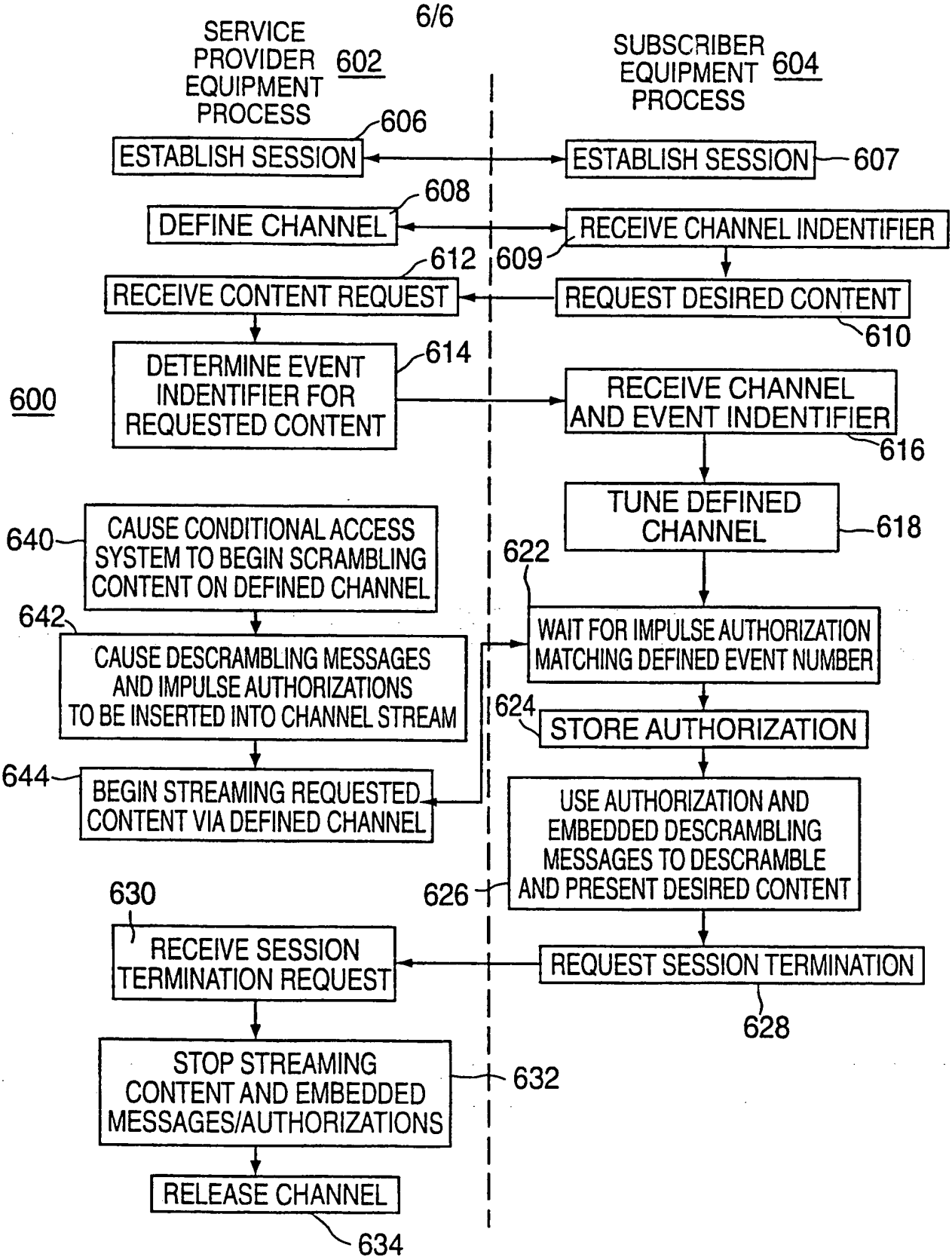


FIG. 6

BNSDOCID: <WO 0059203A2_I_>

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 October 2000 (05.10.2000)

PCT

(10) International Publication Number
WO 00/59203 A3

(51) International Patent Classification[7]: H04N 7/10

(21) International Application Number: PCT/US00/08541

(22) International Filing Date: 30 March 2000 (30.03.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/127,128	31 March 1999 (31.03.1999)	US
60/127,122	31 March 1999 (31.03.1999)	US
09/458,620	10 December 1999 (10.12.1999)	US

(71) Applicant: DIVA SYSTEMS CORPORATION [US/US]; 800 Saginaw Drive, Redwood City, CA 94063 (US).

(72) Inventor: BERTRAM, Michael, C.; 417-17 Camille Circle, San Jose, CA 95134 (US).

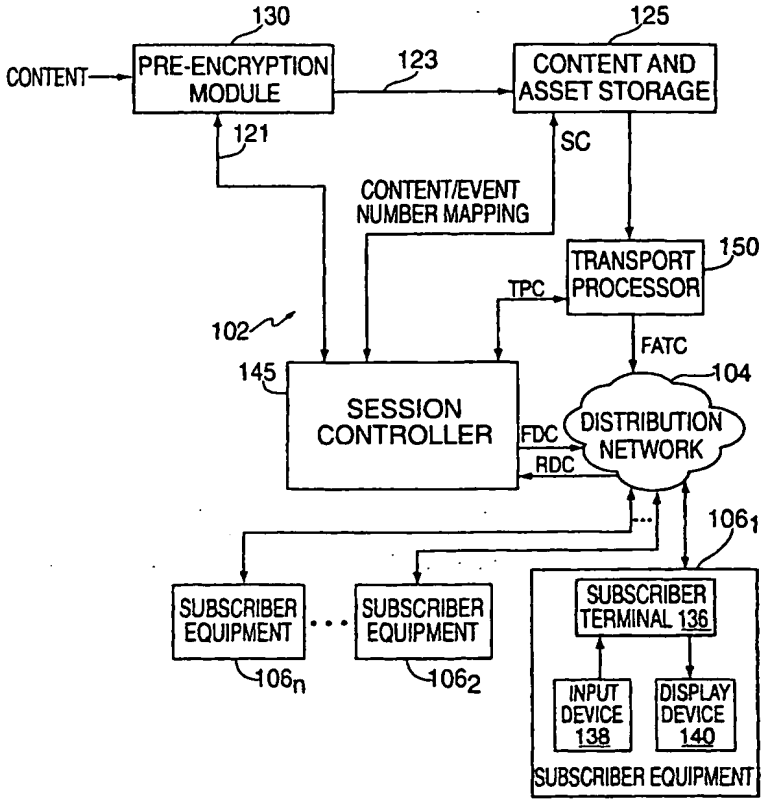
(74) Agents: MOSER, Raymond, R. et al.; Thomason Moser and Patterson LLP, 595 Shrewsbury Avenue, Suite 100, Shrewsbury, New Jersey 07702 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU,

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR PERFORMING IMPULSE AUTHORIZATIONS WITHIN A VIDEO ON DEMAND ENVIRONMENT



(57) Abstract: A method and apparatus (102) for enabling conditional access to on-demand content of variable duration by utilizing either real time encryption of the content or pre-encryption of the content. In either case, embedding decryption messages and impulse authorizations are included with the pre-encrypted information stream.

WO 00/59203 A3

MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

(88) Date of publication of the international search report:
26 April 2001

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/08541

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :348/5.5. 7.
US CL : H04N 7/10
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 348/ 5.5. 6. 7. 10. 12. 13 ; H04N 7/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST TEXT SEARCH

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4,975,951 A (BENNETT) 04 DECEMBER 1990, FIGURES 1-4.	1-13
A	US 5,856,973 A (THOMPSON) 05 JANUARY 1999, FIGURES 1-8.	1-13

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 18 SEPTEMBER 2000	Date of mailing of the international search report 30 OCT 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer NATHAN J. FLYNN Telephone No. (703) 308-6601

Form PCT/ISA/210 (second sheet) (July 1998)*

BNSDOCID: <WO___0059203A3_I_>

This Page Blank (uspto